OFFICE OF INFORMATION SECURITY

[ANALYZED, ANALYSIS INCOMPLETE]: This application has [not] successfully completed the V&V Secure Design Review Validation Process.

Secure Design Review Validation Report

[Application Name] [Application Version]

[Component or Integration Name]

Application-ID: [9D5124EC-2BED-4b47-9F7C-7D930CBE63FC]

Filename: VA SwA Design Validation [Appname] [Appversion] [Date] [ANALYZED, ANALYSIS INCOMPLETE].pdf

MONTH DAY, YEAR

VA

U.S. Department of Veterans Affairs

Office of Information and Technology

Software Assurance Program Office

Table of Contents

1 Secure Design Review Validation Report Introduction

This document contains the results of the validation by the VA Software Assurance Program Office of a developer-performed secure design review of [application name] [component or integration name].

This document contains the following additional sections:

Section 2. Secure Design Review Validation Results

This section summarizes the results of the validation of the developer secure design review.

Section 3. Secure Design Review Validation Process Details

This section describes how the validation of the developer secure design review was performed.

Section 4. Secure Design Review Validation Findings and Recommendations

This section provides residual secure design review validation findings that must be resolved to successfully complete the validation process.[1] This section also provides recommendations for mitigating each category of finding.

Section 5. Secure Design Review Validation Report Conclusion

This section provides a summary of VA application developer responsibilities with respect to the VA Secure Code Review SOP and identifies additional resources for building security in during development.

1.1 Application Information

The version of [application name] (Application-ID [Application-ID]) for which threat modeling tool results were provided was [application version]. The following artifacts were provided by the developer for review:

1. Completed V&V Secure Design Review Validation Request Form
2. [file name] Microsoft Threat Modeling Tool model file
3. [file name] [lists of technologies/libraries utilized document title]
4. [file name] [sequence diagrams document title]
5. [file name] [deployment diagrams document title]
6. [file name] [lists of application interfaces and services utilized document title] [file name]
7. [file name] [other provided document(s) if any]

[1] Per VA OIS Secure Design Review Standard Operating Procedures (SOP), which can be downloaded from https://wiki.mobilehealth.va.gov/display/OISSOFTWARE ASSURANCE/Public+Document+Library

2 Secure Design Review Validation Results

This document contains the results of a Verification and Validation (V&V) review of [application name] [version] [component or integration name], conducted by the VA Software Assurance Program Office, of developer-provided Microsoft Threat Modeling Tool scan result files and supporting documentation. Goals of performing secure design reviews (application threat modeling) at the VA include ensuring that risk-based activities in applications are performed in a secure manner. Goals of V&V secure design review validations include ensuring that secure design reviews performed by VA software developers have been done correctly and consistently.

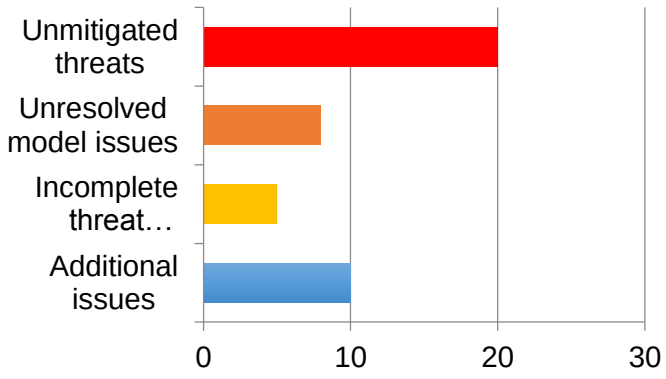
The V&V secure design review validation conducted by the VA Software Assurance Program Office reviewed provided materials to ensure that:

- Application information in secure design review validation request packages was accurate and complete,
- Application secure design review analysis results demonstrate that VA standards have been met, and
- Application secure design review analysis demonstrates that mitigations have been made for issues reported by the Microsoft Threat Modeling Tool, and
- Application secure design review analysis includes justifications for cases where Microsoft Threat Modeling Tool rules are disabled or model analysis results are marked as false positives.

For more information about the validation process, see Section 3.

The V&V secure design review validation conducted by the VA Software Assurance Program Office identified a total of [count] unresolved model issues, [count] unmitigated threats, [count] threats that were not completely analyzed, and [count] additional issues. These issue metrics are depicted in the figure below. For more information about validation results see Section 4.

Figure 1. Summary of Residual Threats & Unresolved Issues



3 Secure Design Review Validation Process Details

The secure design review validation was performed in three basic steps:

Step 1. Perform initial planning

Initial planning includes developing a strategy for performing the review and identifying considerations that should be taken into account during the review, such as any supporting documentation provided by the developer in addition to the Microsoft Threat Modeling file.

Step 2. Review threat model

Reviewing the threat model includes using the Microsoft Threat Modeling Tool together with manual analysis of developer-provided supporting documentation. The VA Software Assurance Program Office reviews the application threat model to ensure that best practices for performing secure design review have been followed by the developer, and that VA standards have been met, as listed in the previous section.

Step 3. Write report

The final step in the secure design review validation process is to capture analysis results in the VA Secure Design Review Validation report, after working with the VA application developer to resolve any issues such as missing validation inputs identified during the review.

3.1 Validation Strategy

The secure code review validation was performed by reviewing Microsoft Threat Modeling Tool files and any supporting documentation provided by the developer. The supporting documentation was reviewed as needed to support analysis of the provided application threat model. The secure design review validation included the following checks, at minimum:

Review developer-provided application threat model for matching documentation

This validation check consists of ensuring the provided documentation is consistent with the uploaded application threat model files. While during the comparison there may be some differences such as document revisions, provided documentation should be up to date and specific to the application being analyzed.

Review developer-provided application threat model for model issues

This validation check consists of reviewing application threat model files for anomalies, e.g. issues reported by the application threat modeling tool that may affect the quality or completeness of the model.

Review developer-provided application threat model for threat analysis issues

This validation check consists of ensuring that there are no unanalyzed or unmitigated threats in the uploaded application threat model file. This includes reviewing mitigation descriptions and supporting documentation as well as any explanations of threats marked as Not Applicable.

Review developer-provided application threat model for suppression of issues

This validation check consists of reviewing application threat model files to ensure that Microsoft Threat Modeling Tool threat generation has not been disabled and that threats generated from the model have not been inappropriately filtered out.

Perform additional supporting analysis, as needed

This validation check consists of performing additional supporting analysis for items that may have been identified during the course of the validation for a particular application.

3.2 Tools Used for Validation

The VA Software Assurance Program Office uses the same application threat modeling tool as VA application developers, in accordance with the VA Secure Design Review SOP. For this validation, Microsoft Threat Modeling Tool version [version] was used.

3.3 Categorization of Findings

The findings that resulted from the secure design review validation are grouped in Section 4 of this report. Findings were rated according to VA Secure Design Review SOP, and/or at the discretion of the VA Software Assurance Program Office as follows:

Findings for unmitigated threats

Unmitigated threats may result in vulnerabilities that vary from lower to higher in severity. For example, unmitigated threats may allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.

Findings for unresolved model issues

This finding categorization is reserved for issues having to do with how the model was developed. For example, model diagram errors. This category also includes issues having to do with documentation inconsistencies.

Findings for incomplete threat analysis

This finding categorization is reserved for issues having to do with how threats were analyzed by the developer. For example, referenced supporting documentation may not have been provided, or may not be relevant for the specific threat. This category also includes issues having to do with suppression of issues.

Additional findings

This finding categorization is reserved for any additional concerns identified by the VA Software Assurance Program Office review that do not correspond to the categories above. For example, new issues may be identified during the course of the validation while reviewing supporting documentation.

4 Secure Design Review Validation Findings and Recommendations

Note: Overall passing verdicts require 0 model issues, 0 potential threats that were not correctly or sufficiently analyzed, and 0 additional issues.

There may be one or more unmitigated confirmed valid threats, but these do not contribute to the overall Analyzed / Analysis Incomplete verdict.

More information about confirmed valid threats to the extent referenced below can be found in the Microsoft Threat Modeling Tool file for this application.

4.1 Unresolved Model Issues ([#] Total)

4.1.1 [Context, Level 0, Level 1, Level 2] Diagram ([#] Total)

Based on the information provided, it does not appear that there were issues with the construction of the application threat model.

Or,

Description of Concern		
There are issues with how the application threat model was finalized by the developer. These issues may have impacted the ability of Microsoft Threat Modeling Tool to accurately identify threats. Descriptions of unresolved model issues are below.		
Issue	**Description**	**Recommendation**
1.		
2.		
3.		
4.		

Or for extreme circumstances as with code review validations,

WARNING: The V&V Secure Design Review Validation Process has encountered blocking issues; current model analysis should not be relied upon.

4.2 Unmitigated Threats ([#] Total)

4.2.1 [Interaction name] Interaction

Based on the information provided by the developer, it does not appear that there are any unmitigated threats that have been identified by the Microsoft Threat Modeling Tool.

Or,

The following threats that have been identified by the Microsoft Threat Modeling Tool have been left unmitigated and are still being reported by Microsoft Threat Modeling Tool:

Threat-ID	Title	Category	Interaction	Description

Or for extreme circumstances as with code review validations,

WARNING: The V&V Secure Design Review Validation Process has encountered blocking issues; current model analysis should not be relied upon.

4.3 Incomplete Threat Analysis ([#] Total)

4.3.1 [Interaction name] Interaction

Based on the information provided, it does not appear that there were any threats with incomplete analysis by the developer.

Or,

Threat-ID	Title	Category	Interaction	Description

Or for extreme circumstances as with code review validations,

WARNING: The V&V Secure Design Review Validation Process has encountered blocking issues; current model analysis should not be relied upon.

4.4 Additional Issues ([#] Total)

4.4.1 [Context, Level 0, Level 1, Level 2] Diagram ([#] Total)

4.4.2 [Interaction name] Interaction

There were no additional findings that were identified during the course of the validation.

Or,

Title	Category
4.4.3 [Title] – [Category] ([#] Instances)	**[Title]**
Description of Concern	
There are concerns related to [title] ([Category]). Individual instances that were found during the secure design review are listed below. A model example, description of potential impact, and recommendations follow.	
Location	
Diagram	**Interaction**	**Description**
1.		
2.		
3.		
4.		
Model Example	
A portion of the application threat model is reproduced below. In the example, [provide a partial screen snap and a brief description].	
Potential Impact	

[Provide description of impact]
Remediation
[Provide remediation advice]

5 Secure Design Review Validation Report Conclusion

Designing secure applications is every VA application developer's responsibility. Application-level vulnerabilities generally manifest themselves as one of two types: **design flaws** introduced by weaknesses during the requirements, design, or architecture phase; or **implementation bugs** introduced by weaknesses during the actual coding of the application.

Microsoft Threat Modeling tool should be used according to the VA Secure Design Review SOP to minimize design flaws during application development. Microsoft Threat Modeling Tool supports the "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege" (STRIDE) threat modeling process. STRIDE is an iterative process where an application's design is systematically decomposed and formulaically analyzed for vulnerabilities.

The VA Software Assurance Program Office uses the same application threat modeling tool (Microsoft Threat Modeling Tool) as VA application developers during the secure design review validation process to ensure consistency and completeness of analysis.

5.1 Related Resources

The following resources may be helpful to readers of this report:

VA Software Assurance Support Site

This site provides VA Software Assurance Program Office resources to assist VA application developers with performing secure code reviews and secure design reviews during development and also during Assessment and Authorization (A&A) and continuous monitoring.

VA Secure Design Review Standard Operating Procedures (SOP)

This document provides establishes policies and procedures for performing secure design review (application threat modeling) of custom-developed applications at the VA.

Microsoft Threat Modeling Tool Site

This site provides information and download information for the Microsoft Threat Modeling Tool.